| | | | |
|---|---|---|---|
| | **LOS LUNAS POLICE DEPARTMENT** | | |
| | ADMINISTRATION | NUMBER: ADM.37.01 | EFFECTIVE DATE: November 22, 2017 |
| | SUBJECT: Criminal Justice Information Service (CJIS) | | REVIEW DATE: November 22, 2017 |
| | AMENDS/ SUPERSEDES: | | NMSA: |
| NMMLEPSC STANDARDS: | APPROVED BY CHIEF OF POLICE NAITHAN G. GURULE  Signature | | |

## 1.0 Physical Protection Policy

### 1.1 Purpose:

The purpose of this policy is to provide guidance for agency personnel, support personnel, and private contractors/vendors for the physical, logical, and electronic protection of Criminal Justice Information (CJI). All physical, logical, and electronic access must be properly documented, authorized and controlled on devices that store, process, or transmit unencrypted CJI. This Physical Protection Policy focuses on the appropriate access control methods needed to protect the full lifecycle of CJI from insider and outsider threats.

This Physical Protection Policy was developed using the FBI's *CJIS Security Policy* 5.1 dated July 13, 2012. The intended target audience is Los Lunas Police Department personnel, support personnel, and private contractor/vendors with access to CJI whether logically or physically. The local agency may complement this policy with a local policy; however, the *CJIS Security Policy* shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the *CJIS Security Policy* standards.

### 1.2 Physically Secure Location:

A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the FBI CJI and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled, and secured. Restricted non-public areas in the Los Lunas Police Department shall be identified with a sign at the entrance.

### 1.3 Visitors Access:

A visitor is defined as a person who visits the Los Lunas Police Department facility on a temporary basis who is not employed by the Los Lunas Police Department and has no unescorted access to the physically secure location within the Los Lunas Police Department where FBI CJI and associated information systems are located. For agencies with jails with CJIS terminals, additional visit specifications need to be established per agency purview and approval.

1.3.1 Visitors shall:

1. Check in before entering a physically secure location by:
   a. Completing the visitor access log, which includes: name and visitor's agency, purpose for the visit, date of visit, time of arrival and departure, name and agency of person visited, and form of identification used to authenticate visitor.
   b. Document badge number on visitor log if visitor badge issued. If Los Lunas Police Department issues visitor badges, the visitor badge shall be worn on approved visitor's outer clothing and collected by the agency at the end of the visit.
   c. Planning to check or sign-in multiple times if visiting multiple physically secured locations and/or building facilities that are not adjacent or bordering each other that each has their own individual perimeter security to protect CJI.
2. Be accompanied by a Los Lunas Police Department escort at all times to include delivery or service personnel. An escort is defined as an authorized personnel who accompanies a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any CJI therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.
3. Show Los Lunas Police Department personnel a valid form of photo identification.

4. Follow Los Lunas Police Department policy for authorized unescorted access.
    a. Noncriminal Justice Agency (NCJA) like city or county IT who require frequent unescorted access to restricted area(s) will be required to establish a Management Control Agreement between the Los Lunas Police Department and NCJA. Each NCJA employee with CJI access will appropriately have state and national fingerprint-based record background check prior to this restricted area access being granted.
    b. Private contractors/vendors who requires frequent unescorted access to restricted area(s) will be required to establish a Security Addendum between the Los Lunas Police Department and each private contractor personnel. Each private contractor personnel will appropriately have state and national fingerprint-based record background check prior to this restricted area access being granted.
5. Not be allowed to view screen information mitigating shoulder surfing.
6. Individuals not having any legitimate business in a restricted area shall be courteously escorted to a public area of the facility. Strangers in physically secure areas without an escort should be challenged. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel shall be notified or call 911.
7. Not be allowed to sponsor another visitor.
8. Not enter into a secure area with electronic devices unless approved by the Los Lunas Police Department Local Area Security Officer (LASO) to include cameras and mobile devices. Photographs are not allowed without permission of the Los Lunas Police Department assigned personnel.
9. All requests by groups for tours of the Los Lunas Police Department facility will be referred to the proper agency point of contact for scheduling. In most cases, these groups will be handled by a single form, to be signed by a designated group leader or representative. Remaining visitor rules apply for each visitor within the group. The group leader will provide a list of names to front desk personnel for instances of emergency evacuation and accountability of each visitor while on agency premises.

**1.4 Authorized Physical Access:**

Only authorized personnel will have access to physically secure non-public locations. The Los Lunas Police Department will maintain and keep current a list of authorized personnel. All physical access points into the agency's secure areas will be authorized before granting access. The agency will implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJI. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.

**1.4.1** All personnel with CJI physical and logical access must:

1. Meet the minimum personnel screening requirements prior to CJI access.
    a. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.
    b. Support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.
    c. Prior to granting access to CJI, the Los Lunas Police Department on whose behalf the contractor is retained shall verify identification via a state of residency and national fingerprint-based record check.
    d. Refer to the *CJIS Security Policy* for handling cases of felony convictions, criminal records, arrest histories, etc.
2. Complete security awareness training.
    a. All authorized Los Lunas Police Department, Noncriminal Justice Agencies (NCJA) like city or county IT and private contractor/vendor personnel will receive security awareness training within six months of being granted duties that require CJI access and every two years thereafter.
    b. Security awareness training will cover areas specified in the *CJIS Security Policy* at a minimum.

3. Be aware of who is in their secure area before accessing confidential data.

a. Take appropriate action to protect all confidential data.

b. Protect all terminal monitors with viewable CJI displayed on monitor and not allow viewing by the public or escorted visitors.

4. Properly protect and not share any individually issued keys, proximity cards, computer account passwords, etc.

    a. Report loss of issued keys, proximity cards, etc to authorized agency personnel.

    b. If the loss occurs after normal business hours, or on weekends or holidays, personnel are to call the Los Lunas Police Department POC to have authorized credentials like a proximity card de-activated and/or door locks possibly rekeyed.

    c. Safeguard and not share passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and all other facility and computer systems security access procedures. See Disciplinary Policy.

5. Properly protect from viruses, worms, Trojan horses, and other malicious code.
6. Web usage—allowed versus prohibited; monitoring of user activity. (allowed versus prohibited is at the agency's discretion)
7. Do not use personally owned devices on the Los Lunas Police Department computers with CJI access. (Agency discretion). See Personally Owned Policy.
8. Use of electronic media is allowed only by authorized Los Lunas Police Department personnel. Controls shall be in place to protect electronic media and printouts containing CJI while in transport. When CJI is physically moved from a secure location to a non-secure location, appropriate controls will prevent data compromise and/or unauthorized access.

9. Encrypt emails when electronic mail is allowed to transmit CJI-related data as such in the case of Information Exchange Agreements.

a. (Agency Discretion for allowance of CJI via email)

b. If CJI is transmitted by email, the email must be encrypted and email recipient must be authorized to receive and view CJI.

10. Report any physical security incidents to the Los Lunas Police Department's LASO to include facility access violations, loss of CJI, loss of laptops, Blackberries, thumb drives, CDs/DVDs and printouts containing CJI.
11. Properly release hard copy printouts of CJI only to authorized vetted and authorized personnel in a secure envelope and shred or burn hard copy printouts when no longer needed. Information should be shared on a "need to know" basis. (See Sanitization and Destruction Policy)
12. Ensure data centers with CJI are physically and logically secure.
13. Keep appropriate Los Lunas Police Department security personnel informed when CJI access is no longer needed. In the event of ended employment, the individual must surrender all property and access managed by the local agency, state and/or federal agencies.

14. Not use food or drink around information technology equipment.

15. Know which door to use for proper entry and exit of the Los Lunas Police Department and only use marked alarmed fire exits in emergency situations.

16. Ensure the perimeter security door securely locks after entry or departure. Do not leave any perimeter door propped opened and take measures to prevent piggybacking entries.

### 1.5 Roles and Responsibilities: Terminal Agency Coordinator (TAC)

The TAC serves as the point-of-contact at the Los Lunas Police Department for matters relating to CJIS information access. The TAC administers CJIS systems programs within the agency and oversees the agency's compliance with FBI and state CJIS systems policies.

### 1.6 Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA (state) approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

### 1.7 Agency Coordinator (AC)

An AC is a staff member of the Contracting Government Agency (CGA) who manages the agreement between the private contractor(s)/vendor(s) and the Los Lunas Police Department. A CGA is a government agency, whether a Criminal Justice Agency (CJA) or a NCJA, that enters into an agreement with a private contractor/vendor subject to the CJIS Security Addendum. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of private contractor/vendor employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

### 1.8 CJIS System Agency Information Security Officer (CSA ISO)

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.
2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting

procedures at the local level. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

### 1.9 Information Technology Support

In coordination with above roles, all vetted IT support staff will protect CJI from compromise at the Los Lunas Police Department by performing the following:

1. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed. Know where CJI is stored, printed, copied, transmitted and planned end of life. CJI is stored on laptops, mobile data terminals (MDTs), computers, servers, tape backups, CDs, DVDs, thumb drives, RISC devices and internet connections as authorized by the Los Lunas Police Department. For agencies who submit fingerprints using Live Scan terminals, only Live Scan terminals that receive CJI back to the Live Scan terminal will be assessed for physical security.
2. Be knowledgeable of required Los Lunas Police Department technical requirements and policies taking appropriate preventative measures and corrective actions to protect CJI at rest, in transit and at the end of life.
3. Take appropriate action to ensure maximum uptime of CJI and expedited backup restores by using agency approved best practices for power backup and data backup means such as generators, backup universal power supplies on CJI-based terminals, servers, switches, etc.
4. Properly protect the Los Lunas Police Department's CJIS system(s) from viruses, worms, Trojan horses, and other malicious code (real-time scanning and ensure updated definitions).
    a. Install and update antivirus on computers, laptops, MDTs, servers, etc.
    b. Scan any outside non-agency owned CDs, DVDs, thumb drives, etc., for viruses, if the Los Lunas Police Department allows the use of personally owned devices. (See the Los Lunas Police Department Personally Owned Device Policy)
5. Data backup and storage—centralized or decentralized approach.
    a. Perform data backups and take appropriate measures to protect all stored CJI.

b. Ensure only authorized vetted personnel transport off-site tape backups or any other media that store CJI that is removed from physically secured location.
c. Ensure any media released from the Los Lunas Police Department is properly sanitized / destroyed. (See Sanitization and Destruction Policy)

6. Timely application of system patches—part of configuration management.
   a. The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.
   b. When applicable, see the Los Lunas Police Department Patch Management Policy.
7. Access control measures
   a. Address least privilege and separation of duties.
   b. Enable event logging of:
      i. Successful and unsuccessful system log-on attempts.
      ii. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.
      iii. Successful and unsuccessful attempts to change account passwords.
      iv. Successful and unsuccessful actions by privileged accounts.
      v. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.
   c. Prevent authorized users from utilizing publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
8. Account Management in coordination with TAC
   a. Agencies shall ensure that all user IDs belong to currently authorized users.
   b. Keep login access current, updated and monitored. Remove or disable terminated or transferred or associated accounts.
   c. Authenticate verified users as uniquely identified.
   d. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs.
   e. Not use shared generic or default administrative user accounts or passwords for any device used with CJI.

f. Passwords
    i. Be a minimum length of eight (8) characters on all systems.
    ii. Not be a dictionary word or proper name.
    iii. Not be the same as the User ID.
    iv. Expire within a maximum of 90 calendar days.
    v. Not be identical to the previous ten (10) passwords.
    vi. Not be transmitted in the clear or plaintext outside the secure location.
    vii. Not be displayed when entered.
    viii. Ensure passwords are only reset for authorized user.

9. Network infrastructure protection measures.
    a. Take action to protect CJI-related data from unauthorized public access.
    b. Control access, monitor, enabling and updating configurations of boundary protection firewalls.
    c. Enable and update personal firewall on mobile devices as needed.
    d. Ensure confidential electronic data is only transmitted on secure network channels using encryption and *advanced authentication when leaving a physically secure location. No confidential data should be transmitted in clear text. *Note: for interim compliance, and for the sole purpose of meeting the advanced authentication policy, a police vehicle shall be considered a physically secure location until September 30th 2013. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods.*
    e. Ensure any media that is removed from a physically secured location is encrypted in transit by a person or network.
    f. Not use default accounts on network equipment that passes CJI like switches, routers, firewalls.
    g. Make sure law enforcement networks with CJI shall be on their own network accessible by authorized personnel who have been vetted by the Los Lunas Police Department. Utilize Virtual Local Area Network (VLAN) technology to segment CJI traffic from other noncriminal justice agency traffic to include other city and/or county agencies using same wide area network.
10. Communicate and keep the Los Lunas Police Department informed of all scheduled and unscheduled network and computer downtimes, all security incidents and misuse. The

ultimate information technology management control belongs to Los Lunas Police Department.

### 1.10 Front desk and Visitor Sponsoring Personnel

Administration of the Visitor Check-In / Check-Out procedure is the responsibility of identified individuals in each facility. In most facilities, this duty is done by the Front desk or Reception Desk.

Prior to visitor gaining access to physically secure area:

1. The visitor will be screened by the Los Lunas Police Department personnel for weapons. No weapons are allowed in the agency except when carried by authorized personnel as deemed authorized by the Los Lunas Police Department.
2. The visitor will be screened for electronic devices. No personal electronic devices are allowed in any agency facility except when carried by authorized personnel as deemed authorized by the Los Lunas Police Department.
3. Escort personnel will acknowledge being responsible for properly evacuating visitor in cases of emergency. Escort personnel will know appropriate evacuation routes and procedures.
4. Escort and/or Front desk personnel will validate visitor is not leaving agency with any agency owned equipment or sensitive data prior to Visitor departure.

All Los Lunas Police Department personnel and supporting entities are responsible to report any unauthorized physical, logical, and electronic access to the Los Lunas Police Department officials. For Los Lunas Police Department, the point of contacts to report any non-secure access is:

| | | |
|---|---|---|
| LASO Name: | LASO Phone: | LASO email: |
| AC Name: | AC Phone: | AC email: |
| State C/ISO Name: | C/ISO Phone: | C/ISO email: |

### 1.11 Penalties:

Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and / or termination.

**Violation of any of the requirements in this policy by any visitor can result in similar disciplinary action against the sponsoring employee, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.**

**Acknowledgement:**

**I have read the policy and rules above and I will:**

- **Abide by the Los Lunas Police Department Physical Protection Policy. I understand any violation of this policy may result in discipline up to and including termination.**
- **Complete the security awareness training and take action to protect the Los Lunas Police Department's facilities, personnel and associated information systems.**
- **Report any unauthorized physical access to the Los Lunas Police Department's LASO.**

**Signature: _____ Date: _____/2012____**

Other Related Policy Reference:

- Sanitization and Destruction Policy
- Disciplinary Policy
- *CJIS Security Policy*

## 2.0 User Account / Access Validation

### 2.1 Purpose:

All accounts shall be reviewed at least every six months by the terminal agency coordinator (TAC) or his/her designee to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain Criminal Justice Information. The TAC may also conduct periodic reviews.

All guest accounts (for those who are not official employees of the CJA) with access to the criminal justice network shall contain an expiration date of one year or the work completion date, whichever

occurs first. All guest accounts (for private contractor personnel) must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

The TAC must disable all new accounts that have not been accessed within 30 days of creation. Accounts of individuals on extended leave (more than 30 days) should be disabled. (Note: Exceptions can be made in cases where uninterrupted access to IT resources is required. In those instances, the individual going on extended leave must have a manager-approved request from the designated account administrator or assistant.)

The TAC must be notified if a user's information system usage or need-to-know changes (i.e., the employee is terminated, transferred, etc.). If an individual is assigned to another office for an extended period (more than 90 days), the TAC will transfer the individual's account(s) to the new office (CJA).

The TAC will remove or disable all access accounts for separated or terminated employees immediately following separation from the agency.

Primary responsibility for account management belongs to the Terminal Agency Coordinator (TAC).

The TAC shall:
- Modify user accounts in response to events like name changes, accounting changes, permission changes, office transfers, etc.,
- Periodically review existing accounts for validity (at least once every 6 months), and
- Cooperate fully with an authorized security team that is investigating a security incident or performing an audit review.

**3.0 Allowed Personally Owned Device**

**3.1 Purpose:**

A personally owned information system or device shall be authorized to access, process, store or transmit Los Lunas Police Department, state, or FBI Criminal Justice Information (CJI) only when these established and documented specific terms and conditions are met. This control does not

apply to the use of personally owned information systems to access the Los Lunas Police Department's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).

This Personally Owned Device Policy was developed using the FBI's *CJIS Security Policy* 5.1 dated July 13, 2012. The intended target audience is Los Lunas Police Department personnel, support personnel and private contractors/vendors. The Los Lunas Police Department may complement this policy with a local policy; however, the *CJIS Security Policy* shall always be the minimum standard and the local policy may augment, or increase the standards, but shall not detract from the *CJIS Security Policy* standards.

### 3.2 Scope:

This policy applies to all Los Lunas Police Department personnel, support personnel, and/or private contractors/vendors who are authorized to use personally owned devices to connect to any physical, logical, and/or electronic premise of the Los Lunas Police Department to access, process, store, and/or transmit CJI. This also includes any private contractors/vendors who will conduct maintenance on any network device that processes, stores, and/or transmits FBI CJI.

### 3.3 Personally Owned Devices:

A personally owned device is any technology device that was purchased by an individual and was not issued by the Los Lunas Police Department. A personal device includes any portable technology like camera, USB flash drives, USB thumb drives, DVDs, CDs, air cards and mobile wireless devices such as Androids, Blackberry OS, Apple iOS, Windows Mobile, Symbian, tablets, laptops or any personal desktop computer. Threats to mobile handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services.

The Los Lunas Police Department will maintain management control and authorize the use of personally owned devices. The Los Lunas Police Department shall develop guidelines to define which employees can use their own devices, the types of devices they can use, and which applications and data they can access, process, or store on their devices.

**3.3.1** Personally owned devices must:

- Be authorized by Los Lunas Police Department to access, process, transmit, and/or store FBI CJI.
- Be inspected by Los Lunas Police Department's IT staff and the LASO to ensure appropriate security requirements on the device are up-to-date and meet the FBI's *CJIS Security Policy* requirements prior to use.
- Take necessary precautions when using device outside of a physically secure area.

  Read below and also see Physical Protection Policy.

**3.4 Remote Access:**

The Los Lunas Police Department shall authorize, monitor, and control all methods of remote access to the information systems that can access, process, transmit, and/or store FBI CJI. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency controlled network (e.g., the Internet).

The Los Lunas Police Department shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The Los Lunas Police Department shall control all remote accesses through managed access control points. The Los Lunas Police Department may permit remote access for privileged functions only for compelling operational needs but shall document the rationale for such access in the security plan for the information system.

Utilizing publicly accessible computers to access, process, store or transmit CJI is prohibited. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

**3.5 Roles and Responsibilities:**

**3.5.1 Owner Role:** The owner agrees to:

1. Follow necessary policy and procedures to protect FBI CJI.
2. Usage of their device will be for work-related purposes.
3. Bring their device to work to use during normal work hours and not share the device with anyone else.
4. Los Lunas Police Department having the authority to erase device remotely as needed.
5. Be responsible for any financial obligations for device.
6. Protect individual's and Los Lunas Police Department's privacy.

7. Use good judgement before installing free applications. Sometimes free applications track your personal information with limited disclosure or authorization, and then sell your profile to advertising companies.
8. Use good judgement on amount of time applied to personal use of personally owned devices during normal work business hours.
9. Access FBI CJI only from an approved and authorized storage device.
10. Do not stream music or videos using personally owned devices when connected to Los Lunas Police Department's network to prevent sluggishness.
11. Report lost or stolen mobile or storage devices to the Los Lunas Police Department's Local Agency Security Officer (LASO) within one business day.
12. Review the use of device alerts and update services to validate you requested them. Restrict notifications not requested by looking at your device's settings.
13. Control wireless network and service connectivity. Validate mobile device default settings are not connecting to nearby Wi-Fi networks automatically. Some of these networks, like in airports or neighborhood coffee shops, may be completely open and unsecure.

## 3.6 Information Technology Role

**3.6.1** The Los Lunas Police Department IT support role shall, at a minimum, ensure that external storage devices:

1. Are encrypted when FBI CJI is stored electronically.
2. Are scanned for virus and malware prior to use and/or prior to being connected to the agency's computer or laptop.

**3.6.2** The Los Lunas Police Department IT support role shall, at a minimum, ensure that all personally owned devices:

1. Apply available critical patches and upgrades to the device operating system.
2. Are kept updated with security patches, firmware updates and antivirus.
3. Are configured for local device authentication.
4. Use advanced authentication and encryption when FBI CJI is stored and/or transmitted.

5. Be able to deliver built-in identity role-mapping, network access control (NAC), AAA (Authentication, Authorization, and Accounting) services, and real-time endpoint reporting.
6. Erase cached information when session is terminated.
7. Employ personal firewalls.
8. Minimize security risks by ensuring antivirus and antimalware are installed, running real time and updated.
9. Be scanned for viruses and malware prior to accessing or connecting to Los Lunas Police Department CJIS network.
10. Configure Bluetooth interface as undiscoverable except as needed for pairing, which prevents visibility to other Bluetooth devices except when discovery is specifically needed.
11. Be properly disposed of at end of life. See Media Disposal Policy. Remove FBI CJI before owner sells their personally owned devices or sends it in for repairs.
12. Evaluate personally owned device age. Older device hardware is too outdated for needed updates. Typical life is two years.
13. Ensure device is compatible with needed network protocols and/or compatible with customized applications developed for access FBI CJI through testing.
14. Deploy Mobile Device Management or SIM card locks and credential functions. The credential functions require a pass code to use Los Lunas Police Department's network services. *(Research enterprise mobile device management solutions- see product working successfully in real life scenario with the type of mobile device your State/Agency wants to use prior to implementing. The enterprise mobile device solution must be compatible with chosen device products.)*
15. Ensure owner and IT staff have mobile backup enabled to an approved Los Lunas Police Department location. Set a daily or weekly schedule to periodically synch data and applications. If backup contains FBI CJI, take appropriate security measures for storage of FBI CJI. See Media Protection Policy.
16. Retain the ability to secure, control and remotely erase agency data on employee-owned devices in the event of a security breach or if the employee leaves the agency employment or the device is lost or stolen. This remote ability can be done through technology that allows virtual access to company applications.
17. Enable mobile device in a "find my phone" service to allow finding device.
18. Consider adding extra protection such as a total device reset if the PIN is guessed incorrectly a certain number of attempts.

19. Be able to easily identify connected users and devices. Track, log and manage every personally used device allowed to connect to agency technology resources for secure FBI CJI access.
20. Perform pre and post-authentication checks.
21. Ability to allow and deny access. Selectively grant proper network access privileges.

### 3.7 Local Area Security Officer (LASO)

The LASO will:

1. Identify who is using the personally owned approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

### 3.8 Penalties

Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and/or termination. Personally owned information technology resources used may be retained by the Los Lunas Police Department for evaluation in investigation of security violations.

Violation of any of the requirements in this policy by any unauthorized person can result in similar disciplinary action against the device owner, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

### 3.9 Acknowledgement:

**The Los Lunas Police Department, agency personnel, IT support, private contractors/vendors, and the LASO alike will agree to commit to all bring your own (BYO) rules.**

**I have read the policy and rules above and I will:**

- **Authorize the Los Lunas Police Department to remotely wipe my mobile device.**
- **Abide by the Los Lunas Police Department Personally Owned Device policy. I understand any violation of this policy may result in discipline up to and including termination.**
- **Complete the security awareness training and take action to protect Los Lunas Police Department facilities, personnel and associated information systems.**
- **Report any unauthorized device access to Los Lunas Police Department LASO.**

**Signature: _____Date:_____/20____**

**Questions**

Any questions related to this policy may be directed to the Los Lunas Police Department's LASO:

| | | |
|---|---|---|
| LASO Name: | LASO Phone: | LASO email: |
| State CSO/ISO Name: | CSO/ISO Phone: | CSO/ISO email: |

Other Related Policy Reference:

- See Media Sanitization and Destruction Policy
- Physical Protection Policy

### 4.0 Media Protection

### 4.1 Purpose:

The intent of the Media Protection Policy is to ensure the protection of the Criminal Justice Information (CJI) until such time as the information is either released to the public via authorized

dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules.

This Media Protection Policy was developed using the FBI's Criminal Justice Information Services (CJIS) Security Policy 5.1 dated 7/13/2012. The *Los Lunas Police Department* may complement this policy with a local policy; however, the CJIS Security Policy shall always be the minimum standard. The local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

### 4.2 Scope:

The scope of this policy applies to any electronic or physical media containing FBI Criminal Justice Information (CJI) while being stored, accessed or physically moved from a secure location from the *Los Lunas Police Department*. This policy applies to any authorized person who accesses, stores, and / or transports electronic or physical media. Transporting CJI outside the agency's assigned physically secure area must be monitored and controlled.

Authorized *Los Lunas Police Department* personnel shall protect and control electronic and physical CJI while at rest and in transit. The *Los Lunas Police Department* will take appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate CJI disclosure and/or use will be reported to the *Los Lunas Police Department* Local Agency Security Officer (LASO). Procedures shall be defined for securely handling, transporting and storing media.

### 4.3 Media Storage and Access:

Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored, or actively being accessed. "Electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" includes printed documents and imagery that contain CJI.

To protect CJI, the *Los Lunas Police Department* personnel shall:

1. Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room.
2. Restrict access to electronic and physical media to authorized individuals.
3. Ensure that only authorized users remove printed form or digital media from the CJI.
4. Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques and procedures. (See Sanitization Destruction Policy)
5. Not use personally owned information system to access, process, store, or transmit CJI unless the *Los Lunas Police Department* has established and documented the specific terms and conditions for personally owned information system usage. (See Personally Owned Device Policy)
6. Not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
7. Store all hardcopy CJI printouts maintained by the *Los Lunas Police Department* in a secure area accessible to only those employees whose job function require them to handle such documents.
8. Safeguard all CJI by the *Los Lunas Police Department* against possible misuse by complying with the Physical Protection Policy, Personally Owned Device Policy, and Disciplinary Policy.
9. Take appropriate action when in possession of CJI while not in a secure area:
    a. CJI must not leave the employee's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.
    b. Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and /or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption.
        i. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.

ii. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

**10.** Lock or log off computer when not in immediate vicinity of work area to protect CJI. Not all personnel have same CJI access permissions and need to keep CJI protected on a need-to-know basis.

**11.** Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of CJI. (See Physical Protection Policy).

### 4.4 Media Transport:

Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. “Electronic media” means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

Dissemination to another agency is authorized if:

1. The other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or
2. The other agency is performing personnel and appointment functions for criminal justice employment applicants.

The *Los Lunas Police Department* personnel shall:

1. Protect and control electronic and physical media during transport outside of controlled areas.
2. Restrict the pickup, receipt, transfer and delivery of such media to authorized personnel.

The *Los Lunas Police Department* personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:

1. Use of privacy statements in electronic and paper documents.
2. Limiting the collection, disclosure, sharing and use of CJI.

3. Following the least privilege and role based rules for allowing access. Limit access to CJI to only those people or roles that require access.
4. Securing hand carried confidential electronic and paper documents by:
    a. Storing CJI in a locked briefcase or lockbox.
    b. Only viewing or accessing the CJI electronically or document printouts in a physically secure location by authorized personnel.
    c. For hard copy printouts or CJI documents:
        i. Package hard copy printouts in such a way as to not have any CJI information viewable.
        ii. That are mailed or shipped, agency must document procedures and only release to authorized individuals. DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL. Packages containing CJI material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery. (Agency Discretion)
5. Not taking CJI home or when traveling unless authorized by *Los Lunas Police Department* LASO. When disposing confidential documents, use a shredder.

### 4.5 Electronic Media Sanitization and Disposal:

The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. Physical media shall be securely disposed of when no longer required, using formal procedures. For end of life media policy, refer to “Sanitization Destruction Policy”.

### 4.6 Breach Notification and Incident Reporting:

The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Incident-related information can be obtained from a

variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

### 4.7 Roles and Responsibilities:

If CJI is improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:

1. *Los Lunas Police Department* personnel shall notify his/her supervisor or LASO, and an incident-report form must be completed and submitted within 24 hours of discovery of the incident. The submitted report is to contain a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident. (Agency Discretion)
2. The supervisor will communicate the situation to the LASO to notify of the loss or disclosure of CJI records.
3. The LASO will ensure the CSA ISO (CJIS System Agency Information Security Officer) is promptly informed of security incidents.
4. The CSA ISO will:
   - **a.** Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.
   - **b.** Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
   - **c.** Act as a single POC for their jurisdictional area for requesting incident response assistance.

### 4.8 Penalties:

Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and / or termination.

### 4.9 Acknowledgement:

**I have read the policy and rules above and I will:**

- **Abide by the *Los Lunas Police Department*'s Media Protection Policy. I understand any violation of this policy may result in discipline up to and including termination.**
- **Report any *Los Lunas Police Department* CJI security incident to Supervisor and / or LASO as identified in this policy.**

**Signature: _____ Date: _____/2012____**

**Questions**

Any questions related to this policy may be directed to the *Los Lunas Police Department*'s LASO:

| | | |
|---|---|---|
| LASO Name: | LASO Phone: | LASO email: |
| State C/ISO Name: | C/ISO Phone: | C/ISO email: |

Other Related Policy Reference:

- See Media Sanitization and Destruction Policy
- Media Disposal Policy
- Physical Protection Policy

### 5.0 Disposal of Media Policy and Procedures

### 5.1 Purpose

The purpose of this policy is to outline the proper disposal of media (physical or electronic) at *Los Lunas Police Department*. These rules are in place to protect sensitive and classified information, employees and *Los Lunas Police Department*. Inappropriate disposal of *Los Lunas Police Department* and FBI Criminal Justice Information (CJI) and media may put employees, *Los Lunas Police Department* and the FBI at risk.

### 5.2 Scope

This policy applies to all *Los Lunas Police Department* employees, contractors, temporary staff, and other workers at *Los Lunas Police Department*, with access to FBI CJIS systems and/or data,

sensitive and classified data, and media. This policy applies to all equipment that processes, stores, and/or transmits FBI CJI and classified and sensitive data that is owned or leased by *Los Lunas Police Department*.

### 5.3 Policy

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store and/or transmit FBI CJI and classified and sensitive data shall be properly disposed of in accordance with measures established by *Los Lunas Police Department*.

Physical media (print-outs and other physical media) shall be disposed of by one of the following methods:

1) Shredding using *Los Lunas Police Department* issued shredders.
2) Placed in locked shredding bins for *a private contractor* to come on-site and shred, witnessed by *Los Lunas Police Department* personnel throughout the entire process.
3) Incineration using *Los Lunas Police Department* incinerators or witnessed by *Los Lunas Police Department* personnel onsite at agency or at contractor incineration site, if conducted by non-authorized personnel.

Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier Hard-drives, etc.) Shall be disposed of by one of the <Agency Name> methods:

1) **Overwriting (at least 3 times)** - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.

2) **Degaussing -** a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.

3) **Destruction –** a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

IT systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from *Los Lunas Police Department*'s control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

### 5.4 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination.

## 6.0 CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SYSTEMS USER AGREEMENT

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities, as well as the noncriminal justice community, for licensing and employment purposes. These services are administered and maintained by the FBI CJIS Division and managed in cooperation with the CJIS Systems Agency (CSA) and its administrator for CJIS data, the CJIS Systems Officer (CSO). The CJIS Systems include, but are not limited to: the Interstate Identification Index (III); National Crime Information Center (NCIC); Uniform Crime Reporting (UCR), whether summary or incident-based reporting to the National Incident-Based Reporting System; Fingerprint Identification Record System; Law Enforcement National Data Exchange (N-DEx); Law Enforcement Online; and the National Instant Criminal Background Check System (NICS).

The FBI CJIS Division provides the following services to its users, as applicable:

1. Operational, technical, and investigative assistance.

2. Telecommunication lines to state, federal, and regulatory interfaces.

3. Legal and legislative review of matters pertaining to all CJIS Systems.

4. Timely information on all aspects of all CJIS Systems and other related programs by means of operating manuals, code manuals, technical and operational updates, various newsletters, information letters, frequently asked questions, and other relevant documents.

5. Training assistance and up-to-date materials provided to each CSO, NICS Point of Contact (POC), state Compact Officer, State Administrator, Information Security Officer (ISO), and other appropriate personnel.

6. Ongoing assistance to Systems' users through meetings and briefings with the CSO**s**, State Administrators, Compact Officers, ISOs, and NICS State POCs to discuss operational and policy issues.

7. Advisory Process through which authorized users have input as to the policies and procedures governing the operation of CJIS programs.

8. National Crime Prevention and Privacy Compact Administrative Office through which states and other authorized users may submit issues concerning the noncriminal justice use of the III System.

9. Annual NICS Users Conference.

10. Audit.

11. Staff research assistance.

**6.1 PART I**

The purpose behind a designated CSO is to unify responsibility for Systems user discipline and to ensure adherence to established procedures and policies within each signatory state/territory/tribal agency and by each federal user. This agreement outlines the responsibilities of each CSO as they relate to all CJIS Systems and other related CJIS administered programs. These individuals are

ultimately responsible for planning necessary hardware, software, funding, and training for access to all CJIS Systems.

To ensure continued access as set forth above, the CSA agrees to adhere to all applicable CJIS policies including, but not limited to, the following:

1. The signatory state/tribal agency will provide fingerprints that meet submission criteria for all qualifying arrests. In addition, states/tribal agencies will make their records available for interstate exchange for criminal justice and other authorized purposes unless restricted by state/tribal law, and, where applicable, continue to move toward participation in the III and, upon ratification of the National Crime Prevention and Privacy Compact, the National Fingerprint File.
2. Appropriate and reasonable quality assurance procedures; e.g., hit confirmation, audits for record timeliness, and validation, must be in place to ensure that only complete, accurate, and valid information is maintained in the CJIS Systems.
3. Biannual file synchronization of information entered into the III by participating states.
4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history records. Additionally, each CSO must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.
5. Audit - Each agency shall be responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO’s lines.
6. Training - Each agency shall be responsible for training requirements, including compliance with operator training mandates.
7. Integrity of the Systems - Each agency shall be responsible for maintaining the integrity of the system in accordance with FBI CJIS Division/state/federal/tribal policies to ensure only authorized terminal access; only authorized transaction submission; and proper handling

and dissemination of CJIS data. Each agency shall also be responsible for computer security incident reporting as required by the *CJIS Security Policy*.

The following documents are incorporated by reference and made part of this agreement for CSA users:

1. Bylaws for the CJIS Advisory Policy Board and Working Groups.

2. CJIS Security Policy.

3. Interstate Identification Index Operational and Technical Manual, National Fingerprint File Operations Plan, NCIC 2000 Operating Manual, UCR Handbook-NIBRS Edition, and National Incident-Based Reporting System Volumes 1, 2, and 4.

4. National Crime Prevention and Privacy Compact, 42 United States Code (U.S.C.) §14616.

5. NCIC Standards and UCR Standards, as recommended by the CJIS Advisory Policy Board.

6. The National Fingerprint File Qualification Requirements.

7. Title 28, Code of Federal Regulations, Parts 20 and 25, §50.12, and Chapter IX.

8. Electronic Fingerprint Transmission Specifications.

9. Other relevant documents, to include: NCIC Technical and Operational Updates, CJIS Information Letters, NICS User Manual, NICS Interface Control Document.

10. Applicable federal, state, and tribal laws and regulations.

**6.2 PART 2**

Additionally, there are authorized federal regulatory recipients and other authorized users that provide electronic fingerprint submissions through a CJIS Wide Area Network (WAN) connection (or other approved form of electronic connection) to the CJIS Division that are required to comply with the following CJIS policies:

1. The authorized user will provide fingerprints that meet submission criteria and apply appropriate and reasonable quality assurance procedures.

2. Security - Each agency is responsible for appropriate security measures as applicable to physical security of communication equipment; personnel security to include background screening requirements; technical security to protect against unauthorized use; and security of criminal history records.

3. Audit - Each authorized user shall be responsible for complying with all audit requirements for CJIS Systems. Additionally, each authorized user is subject to a triennial audit by the CJIS Division Audit staff.

4. Training - Each authorized user receiving criminal history record information shall be responsible for training requirements, including compliance with proper handling of criminal history records.

The following documents are incorporated by reference and made part of this agreement for non-CSA authorized users:

1. CJIS Security Policy.
2. National Crime Prevention and Privacy Compact, 42 U.S.C. §14616.

3. Title 28, Code of Federal Regulations, Parts 20 and 25, § 50.12, and Chapter IX.

4. Other relevant documents, to include CJIS Information Letters.

5. Applicable federal, state, and tribal laws and regulations.

## 6.3 GENERAL PROVISIONS

Funding:
Unless otherwise agreed in writing, each party shall bear its own costs in relation to this agreement. Expenditures will be subject to federal and state budgetary processes and availability of funds pursuant to applicable laws and regulations. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

Termination:

1. All activities of the parties under this agreement will be carried out in accordance to the above-described provisions.

2. This agreement may be amended or terminated by the mutual written consent of the parties authorized representatives.

3. Either party may terminate this agreement upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

   a. The parties will continue participation, financial or otherwise, up to the effective date of termination.

   b. Each party will pay the costs it incurs as a result of termination.

   c. All information and rights therein received under the provisions of this agreement prior to the termination will be retained by the parties, subject to the provisions of this agreement.

## 6.4 ACKNOWLEDGMENT AND CERTIFICATION

As a CSO or CJIS WAN Official (or other CJIS authorized official), I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS Systems users to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in, or obtained by means of, the CJIS Systems. I further acknowledge that failure to comply with these duties and responsibilities may result in the imposition of sanctions against the offending state/agency; other federal, tribal, state, and local criminal justice users; and approved noncriminal justice users with System access, whether direct or indirect. The Director of the FBI (or the National Crime Prevention and Privacy Compact Council), may approve sanctions to include the termination of CJIS services.

I hereby certify that I am familiar with all applicable documents that are made part of this agreement and to all applicable federal and state laws and regulations relevant to the receipt and dissemination of documents provided through the CJIS Systems.
This agreement is a formal expression of the purpose and intent of both parties and is effective when signed. It may be amended by the deletion or modification of any provision contained therein, or by the addition of new provisions, after written concurrence of both parties. The “Acknowledgment and Certification” is being executed by the CSO or CJIS WAN Official (or other CJIS authorized official) in both an individual and representative capacity**.** Accordingly, this agreement will remain in effect after the CSO or CJIS WAN Official (or other CJIS authorized official) vacates his/her position or until it is affirmatively amended or rescinded in writing. This agreement does not confer, grant, or authorize any rights, privileges, or obligations to any third party.

## 6.5 SYSTEMS USER AGREEMENT

Please execute either Part 1 or Part 2

**PART 1**

_____ Date: _____

CJIS Systems Officer

_____

Printed Name/Title

CONCURRENCE OF CSA HEAD:

_____ Date: _____

CSA Head

_____

Printed Name/Title

**PART 2**

_____ Date: _____

CJIS WAN Official (or other CJIS Authorized Official)

_____

Printed Name/Title

CONCURRENCE OF CJIS WAN AGENCY HEAD:

_____ Date: _____

CJIS WAN Agency Head

_____

Printed Name/Title

**FBI CJIS DIVISION**:

_____ Date: _____

[Name]

Assistant Director

FBI CJIS Division

* The FBI Designated Federal Officer should be notified when a CSO or other CJIS WAN/authorized Official vacates his/her position. The name and telephone number of the Acting CSO or other CJIS WAN/authorized Official, and when known, the name and telephone number of the new CSO or other CJIS WAN/authorized Official, should be provided. Revised: 05/03/2006

## 7.0 DISCIPLINARY POLICY

In support of *Los Lunas Police Department*'s mission of public service to the Village of Los Lunas citizens, the *Los Lunas Police Department* provides the needed technological resources needed for personnel to access FBI CJIS systems and information in support of the agency's mission. All agency personnel, with access to FBI Criminal Justice Information (CJI) or any system with stored FBI CJI, have a duty to protect the system and related systems from physical and environmental damage and are responsible for correct use, operation, care and maintenance of the information. All technology equipment: computers, laptops, software, copiers, printers, terminals, MDTs, mobile devices, live scan devices, fingerprint scanners, software to include RMS/CAD, operating systems, etc., used to process, store, and/or transmit FBI CJIS is a privilege allowed by *Los Lunas Police Department*, state CSO, and the FBI. To maintain the integrity and security of the *Los Lunas Police Department*'s and FBI's CJIS systems and data, this computer use privilege requires adherence of relevant federal, state and local laws, regulations and contractual obligations. All existing laws and *Los Lunas Police Department* regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply to personal conduct.

Misuse of computing, networking or information resources may result in temporary or permanent restriction of computing privileges up to employment termination. In some misuse situations, account privileges will be suspended to prevent ongoing misuse while under investigation. Additionally, misuse can be prosecuted under applicable statutes. All files are subject for search. Where follow-up actions against a person or agency after an information security incident involves legal action (either civil or criminal), the evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). Complaints alleging misuse of *Los Lunas Police*

*Department*'s computing and network resources and FBI CJIS systems and/or data will be directed to those responsible for taking appropriate disciplinary action.

### *Examples of Misuse with access to FBI CJI*

1. Using someone else's login that you are not the owner.
2. Leaving computer logged in with your login credentials unlocked in a physically unsecure location allowing anyone to access *Los Lunas Police Department* systems and/or FBI CJIS systems and data in your name.
3. Allowing unauthorized person to access FBI CJI at any time for any reason. Note: Unauthorized use of the FBI CJIS systems is prohibited and may be subject to criminal and/or civil penalties.
4. Allowing remote access of *Los Lunas Police Department* issued computer equipment to FBI CJIS systems and/or data without prior authorization by *Los Lunas Police Department*.
5. Obtaining a computer account that you are not authorized to use.
6. Obtaining a password for a computer account of another account owner.
7. Using the *Los Lunas Police Department*'s network to gain unauthorized access to FBI CJI.
8. Knowingly performing an act which will interfere with the normal operation of FBI CJIS systems.
9. Knowingly propagating a computer virus, Trojan horse, worm and malware to circumvent data protection or compromising existing security holes to FBI CJIS systems.
10. Violating terms of software and / or operating system licensing agreements or copyright laws.
11. Duplication of licensed software, except for backup and archival purposes that circumvent copyright laws for use in *Los Lunas Police Department*, for home use or for any customer or contractor.
12. Deliberately wasting computing resources to include streaming audio, videos for personal use that interferes with *Los Lunas Police Department* network performance.
13. Using electronic mail or instant messaging to harass others.
14. Masking the identity of an account or machine.
15. Posting materials publicly that violate existing laws or *Los Lunas Police Department*'s codes of conduct.
16. Attempting to monitor or tamper with another user's electronic mail or files by reading, copying, changing, or deleting without explicit agreement of the owner.
17. Using *Los Lunas Police Department*'s technology resources to advance unwelcome solicitation of a personal or sexual relationship while on duty or through the use of official capacity.
18. Unauthorized possession of, loss of, or damage to *Los Lunas Police Department*'s technology equipment with access to FBI CJI through unreasonable carelessness or maliciousness.

19. Maintaining FBI CJI or duplicate copies of official *Los Lunas Police Department* files in either manual or electronic formats at his or her place of residence or in other physically non-secure locations without express permission.
20. Using *Los Lunas Police Department*'s technology resources and/or FBI CJIS systems for personal or financial gain.
21. Deliberately failing to report promptly any known technology-related misuse by another employee that may result in criminal prosecution or discipline under this policy.
22. Using personally owned devices on *Los Lunas Police Department*'s network to include personally-owned thumb drives, CDs, mobile devices, tablets on wifi, etc. Personally owned devices should not store *Los Lunas Police Department* data, State data, or FBI CJI.

The above listing is not all-inclusive and any suspected technology resource or FBI CJIS system or FBI CJI misuse will be handled by Los Lunas Police Department on a case by case basis. Activities will not be considered misuse when authorized by appropriate Los Lunas Police Department officials for security or performance testing.

**Privacy Policy**

All agency personnel utilizing agency-issued technology resources funded by *Los Lunas Police Department* expressly acknowledges and agrees that such service, whether for business or personal use, shall remove any expectation of privacy. Use of *Los Lunas Police Department* systems indicates consent to monitoring and recording. The *Los Lunas Police Department* reserves the right to access and audit any and all communications including electronic and physical media at rest, in transit and at end of life. *Los Lunas Police Department* personnel shall not store personal information with an expectation of personal privacy that are under the control and management of *Los Lunas Police Department*.

**Personal Use of Agency Technology**

The computers, electronic media and services provided by *Los Lunas Police Department* are primarily for business use to assist personnel in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their business purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

**Misuse Notification**

Due to the increase in the number of accidental or malicious computer attacks against both government and private agencies, *Los Lunas Police Department* shall: (i) establish an operational incident handling capability for all information systems with access to FBI CJIS systems and data. This includes adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities. ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level.

All *Los Lunas Police Department* personnel are responsible to report misuse of *Los Lunas Police Department* technology resources to appropriate *Los Lunas Police Department* officials.

Local contact-LASO: firstnamelast@agencyname.com Phone:

State contact-CSA ISO: firstnamelast@state.gov Phone:

I have read the policy and rules above and I will abide in the *Los Lunas Police Department*'s Disciplinary policy.

Signature: _____ Date: _____/20____